الموضوع: محاضرة 5 نظري 2018/4/26
الفصل الثاني
الخميس

التطابقات الخطية

تعريف: التطابق الخطي هو معادلة من الشكل $ax \equiv b \pmod m$ [1]

حيث a, b أعداد صحيحة معطاة $\in Z$ و m عدد صحيح موجب بحيث $(m \in Z, m > 1)$

$x \in Z$ مجهول نبحث عنه (إذا كان بالإمكان إيجاده)

حل التطابق: هو العدد الصحيح الذي ينتمي لـ Z ويحقق هذا التطابق.

نفرض أن x_0 حل للتطابق $\Leftrightarrow m \mid (ax_0 - b)$

$\Leftrightarrow \exists y \in Z ; my = ax_0 - b$

$\Leftrightarrow b = ax_0 + (-m)y$ [2]

وهذه عبارة عن عبارة ديوفانتية (ديوفانتس).

أي أن مسألة حل التطابق الخطي تؤول إلى مسألة حل عبارة ديوفانتية.

ملاحظة: تعتبر الحلول المتطابقة بالمقاس (m) للتطابق الخطي حلاً واحداً؟

مثال: $3x \equiv 9 \pmod{12}$

ليسا مختلفين لأنهما يقعان بنفس صف تكافؤ 3 فهما حل واحد } $x = 3$ حل لهذا التطابق، $x = -9$ حل للتطابق

$(-27 = (-3)(12) + 9)$ $(-27 - 9 = (-3)(12))$

لذلك نعني بعدد الحلول للتطابق الخطي [1] عدد الحلول الغير متطابقة بالمقاس m.

وبما أن حل التطابق [1] يكافئ حل معادلة ديوفانتس [2]

وكما نعلم أن [2] لها حلول إذا وفقط إذا كان القاسم المشترك الأعظم $d(a, -m) = d(a, m)$ يقسم b.

مبرهنة: يكون للتطابق الخطي $ax \equiv b \pmod m$

حل إذا وفقط إذا كان $d(a, m)$ يقسم b

$d = d(a, m) \mid b$

وعندئذ يوجد للتطابق عدد d من الحلول المختلفة (غير متطابقة) بالمقاس m

تعطى بالعلاقات الآتية:

$x = x_0 + \frac{m}{d} t \quad ; (t = 0, 1, 2, \ldots, d-1)$

نتيجة: إذا كان $d(a, m) = 1$ و m, a أوليان فيما بينهما

فالتطابق الخطي المعطى له حل وحيد

الموضوع :

- إذا كان p عدد أولي لا يقسم a فالتطابق $ax \equiv b (\mod p)$ له حل وحيد لأنه يحقق (القاسم المشترك (1))

بعض الأمثلة

① عين (إن وجدت) حلول التطابق : $6x \equiv 2 (\mod 9)$

نلاحظ أن $d(6,9) = 3 \nmid 2$ فليس للتطابق حل

$9x \equiv 21 (\mod 30)$

$d(9,30) = 3 \mid 21$

يوجد حل للتطابق وبالضبط يوجد 3 حلول غير متطابقة بالمقاس (30)

* باختصار طرفي التطابق مع المقاس على $(d=3)$ نحصل على التطابق الآتي :

$3x \equiv 7 (\mod 10)$

ولأن $d(3,10)=1$ فهو حل للتطابق الناتج حل وحيد.

$\bar{9}$ in Z_{10}

$3[9]=27 \equiv 7 (\mod 10)$

* نلاحظ بالتجريب أن $x=9$ تحقق التطابق

أي $x_0 \equiv 9 (\mod 10)$ حل

$\bar{9} = \{9+10t , t \in Z\}$ وهو يحقق التطابق الأصلي.

وتكون الحلول الثلاثة هي $(x = x_0 + 10t ; t = 0,1,2)$ $(d-1)$ بالمقاس 30

$x = 9 + 10 \cdot 0 = 9$

$= 9 + 10 \cdot 1 = 19$

$= 9 + 10 \cdot 2 = 29$

(?)

$U(Z_{10}) = \{1,3,7,9\}$

$3x \equiv 7 (\mod 10)$

$x \equiv (3)^{-1} 7 (\mod 10)$

$x \equiv 7 \cdot 7 (\mod 10)$

$x \equiv 9 (\mod 10)$

مثال $15x \equiv 60 \pmod{20}$

ملاحظات: $d(15, 20) = 5 \mid 60$

. يوجد حلول للتطابق المعطى وعددها 5 حلول غير متطابقة (مختلفة) بالمقياس 20
. لإيجادها: نقسم التطابق على $d=5$ نحصل على تطابق آخر.

$3x \equiv 12 \pmod{4}$

$x \equiv (3)^{-1}$ in $\mathbb{Z}_4$

$x^{-1} = (3)$

$\Rightarrow x \equiv (3).12 \pmod{4}$

$x \equiv 36 \pmod{4}$

وجواب الحلول $\boxed{x \equiv 0 \pmod{4}}$

$x = x_0 + \frac{20}{5}t \quad ; t = 0, 1, 2, 3, 4$

$x_0 = \bar{0} \qquad x_1 = \bar{4} \qquad x_2 = \bar{8} \qquad x_3 = 12 \qquad x_4 = 16$

تمرين حل المثال الأول $9x \equiv 21 \pmod{30}$ بطريقة ديوفانتس.

$x = -21 \Leftrightarrow 9$

$x = -11 \Leftrightarrow 19$

$x = -1 \Leftrightarrow 29 \quad (29 + \boxed{1} \cdot 30)$

$29 \equiv -1 \pmod{30}$

1 1

الموضوع:

الكسور البسيطة المستمرة المنتهية:

إن إيجاد حلول المعادلات الخطية باستخدام خوارزمية اقليدس أو بالتجريب تصبح طويلة أو متعذرة حين يكون المعامل كبيراً.
لذا نستخدم طريقة الكسور البسيطة المستمرة المنتهية.

تعريف الكسر البسيط المستمر المنتهي: هو كل كسر يكتب على النحو الآتي:

$$\frac{A}{B} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots\, a_{n-1} + \cfrac{1}{a_n}}}}$$

حيث: $a_2, a_3, \dots, a_{n-1}, a_n \in \mathbb{Z}^+$ (+) ، $a_1 \in \mathbb{Z}$ (0 ±)

$\boxed{\mathbb{Z}^+ \ni a_i \;\; i \geq 2}$

ويرمز له بـ:

$$\frac{A}{B} = \langle a_1, a_2, \dots, a_{n-1}, a_n \rangle$$

والمثال يوضح ذلك: اكتب الكسر $\frac{32}{19}$

$\boxed{32 = 1.(19) + 13}$

$$\frac{32}{19} = 1 + \frac{13}{19}$$

$$= 1 + \frac{1}{\left(\frac{19}{13}\right)} = 1 + \frac{1}{1 + \left(\frac{6}{13}\right)} = 1 + \frac{1}{1 + \frac{1}{\left(\frac{13}{6}\right)}} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6}}}$$

$$\frac{32}{19} = \langle 1, 1, 2, 6 \rangle$$

مثال: اكتب الكسر $-\frac{5}{4}$

$\boxed{-5 = (-2)(4) + 3}$

$$-\frac{5}{4} = -2 + \frac{3}{4}$$

$$= -2 + \frac{1}{\frac{4}{3}} = -2 + \frac{1}{1 + \frac{1}{3}}$$

$$-\frac{5}{4} = \langle -2, 1, 3 \rangle$$

تعريف: يسمى العدد (a_k) النسبة الجزئية من المرتبة K وإذا توقفنا بالكسر عند النسبة الجزئية فنحصل على التقريب من المرتبة K الذي يرمز له بـ C_K

أي

$$C_1 = a_1$$

$$C_2 = a_1 + \frac{1}{a_2}$$

$$C_3 = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}$$

$$C_k = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots\, a_{k-1} + \cfrac{1}{a_k}}}$$

مبرهنة: إذا كان لدينا الكسر البسيط المستمر المنتهي $\langle a_1, a_2, a_3, \dots, a_{n-1}, a_n \rangle$ وإذا عرفنا الرموز الآتية:

$$p_1 = a_1 \qquad q_1 = 1$$

$$p_2 = a_1 \cdot a_2 + 1 \qquad q_2 = a_2$$

$$p_3 = a_3 \cdot p_2 + p_1 \qquad q_3 = a_3 \cdot q_2 + q_1$$

$$p_i = a_i p_{i-1} + p_{i-2} \qquad q_i = a_i q_{i-1} + q_{i-2}$$

$$p_n = a_n p_{n-1} + p_{n-2} \qquad q_n = a_n \cdot q_{n-1} + q_{n-2}$$

فإن التقريب من المرتبة (n) للكسر (C_n) المعطى يساوي $C_n = \frac{p_n}{q_n}$ ؛ $n \geq 1$

مبرهنة: من أجل $n \geq 2$ وبنفس الرموز في المبرهنة السابقة تكون العلاقة الآتية صحيحة:

$$p_n \cdot q_{n-1} - p_{n-1} q_n = (-1)^n$$

تعريف المقلوب الضربي: نقول أن $\bar{a}' = a^*$ هو النظير الضربي للعدد الصحيح a بالمقاس m إذا وفقط إذا كان

$$a a^* \equiv 1 \pmod m \iff \text{in } \mathbb{Z}_m \quad \bar{a} \cdot \bar{a}^* = \bar{1}$$

- يكون للعدد الصحيح a نظير ضربي بالمقاس m إذا وفقط إذا كان

$$d(a, m) = 1$$

$$U(\mathbb{Z}_m) = \{\bar{a} \in \mathbb{Z}_m : d(a, m) = 1\}$$

(هي وفقط هي التي صفوف تواقعها أولية مع m)

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17

/ /

الموضوع:

$(\bar{5})^{-1}$ in Z_{11}

يمكنك ملاحظة أن النظير الضربي للعدد 5

بالمقياس 11

هو $\bar{9}$ $\bar{9}\,\bar{5} = \bar{1}$

حل جملة تطابقات خطية:

لتكن جملة التطابقات الخطية $b_i x \equiv a_i \pmod{m_i}$

نقول أن العدد الصحيح x حل مشترك لجملة التطابقات إذا حقق جميع التطابقات المعطاة معاً.

مبرهنة الباقي الصينية:

إذا كانت التطابقات $(m_1, m_2, \dots m_k)$ أولية نسبياً مثنى مثنى

فيوجد لجملة التطابقات $x \equiv a_i \pmod{m_i}$ $(i = 1 \dots k)$

حل وحيد بالمقياس m $m = m_1 \cdot m_2 \cdots m_k$

ويعطى بالعلاقة الآتية:

$$x = [m'_1 M_1 a_1 + m'_2 M_2 a_2 + \dots m'_k M_k a_k] \pmod{m}$$

حيث $M_i = \frac{m}{m_i}$

(m'_i النظير الضربي لـ M_i بالمقياس m_i) $m'_i M_i \equiv 1 \pmod{m_i}$

$$m'_i = (M_i)^{-1} \text{ in } Z_{m_i}$$

مثال: أوجد أصغر عدد صحيح باقي قسمته على 6 يساوي ② وباقي قسمته على 5 يساوي ③ وباقي قسمته على 11 يساوي ⑦

$$\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 3 \pmod{5} \\ x \equiv 7 \pmod{11} \end{cases}$$

ضرب (باقي قسمة ضعفه على 6 يساوي 2 نكتب $2x$)

أو جمع

$3 + x \equiv 2 \pmod{6}$
$x \equiv -1 \pmod{6}$
$x \equiv 5$

نلاحظ أن:

$m_1 = 6$
$m_2 = 5$
$m_3 = 11$

ج/ نسبياً مثنى مثنى وبالتالي يمكن تطبيق مبرهنة الباقي الصينية لجملة التطابقات (حل وحيد)

$$m = 6 \cdot 5 \cdot 11 = 330$$

$$M_1 = \frac{330}{6} = 55$$

$$M_2 = \frac{330}{5} = 66$$

$$M_3 = \frac{330}{11} = 30$$

$$m'_1 M_1 \equiv 1 \pmod 6 \Rightarrow m'_1 \cdot 55 \equiv 1 \pmod 6$$

$$m'_1 \cdot 1 \equiv 1 \pmod 6 \Rightarrow \boxed{m'_1 \equiv 1 \pmod 6}$$

$$m'_2 M_2 \equiv 3 \pmod 5 \Rightarrow m'_2 \cdot 66 \equiv 1 \pmod 5$$

$$\boxed{m'_2 \equiv 1 \pmod 5}$$

$$m'_3 M_3 \equiv 7 \pmod{11} \Rightarrow m'_3 \cdot 30 \equiv 1 \pmod{11}$$

$$m'_3 (8) \equiv 1 \pmod{11} \Rightarrow m'_3 \equiv (8)^{-1} \cdot 1 \pmod{11}$$

$$\boxed{\bar{8} \cdot \boxed{\bar{7}} = \bar{1}} \qquad \Rightarrow \boxed{m'_3 \equiv 7 \pmod{11}}$$

وبالتالي يكون الحل (x)

$$x \equiv [1 \cdot 55 \cdot 2 + 1 \cdot 66 \cdot 3 + 7 \cdot 30 \cdot 7] \pmod{330}$$

$$= [110 + 198 + 1470] \pmod{330}$$

$$= [1778] \pmod{330}$$

$$1 \equiv (128) \pmod{330} \Rightarrow \boxed{x = 128}$$

تمرين: أوجد حل التطابق $19x \equiv 1 \pmod{140}$ بطريقتين.

① طريقة أخذ نظير أولي للعدد   ② طريقة الباقي الصينية.

من أجل طريقة الباقي الصينية نحلل (140) إلى عوامل أولية مثنى مثنى فيما بينها $(140 = 4 \cdot 5 \cdot 7)$ ومن ثم التطابق السابق يكافئ جملة التطابقات:

$$\left.\begin{aligned} 19x &\equiv 1 \pmod 4 \\ 19x &\equiv 1 \pmod 5 \\ 19x &\equiv 1 \pmod 7 \end{aligned}\right\} \Leftrightarrow \left.\begin{aligned} 3x &\equiv 1 \pmod 4 \\ 4x &\equiv 1 \pmod 5 \\ 5x &\equiv 1 \pmod 7 \end{aligned}\right\} \Rightarrow$$

$$\left.\begin{aligned} x &\equiv (3)^{-1} \cdot 1 \pmod 4 \\ x &\equiv (4)^{-1} \cdot 1 \pmod 5 \\ x &\equiv (5)^{-1} \cdot 1 \pmod 7 \end{aligned}\right\} \Leftrightarrow \begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

نكمل باستخدام مبرهنة الباقي الصينية

/ /

الموضوع:

مبرهنة فيرما الصغرى:

إذا كان p عدداً أولياً لا يقسم العدد الصحيح a $(p \nmid a)$
فعندئذٍ، $d(p,a)=1$ و $a^{p-1} \equiv 1 \pmod p$ $[2^{2} = 1 \pmod 3]$

الإثبات:
$(Z_p, +, \cdot)$

$Z_p = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1}\}$

فحقل زمرته الضربية، $U(Z_p) = \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{p-1}\}$

ومن ثم،

$|U(Z_p)| = p-1$

مبرهنة لاغرانج: $|G| = n$، $x \in G : x^n = e$

ومن ثم حسب مبرهنة لاغرانج ونتائجها يكون:

$\bar{a} \in U(Z_p) \Rightarrow (\bar{a})^{p-1} = \bar{1}$

$\Rightarrow (\overline{a^{p-1}}) = \bar{1}$

أي $p \nmid a$ $d(p,a)=1$ فعندئذٍ: $\bar{a} \in U(Z_p)$

ومن ثم $(\bar{a})^{p-1} = \bar{1} \Rightarrow (\overline{a^{p-1}}) = \bar{1}$

بالانتقال إلى التطابقات نحصل على أن:

$a^{p-1} \equiv 1 \pmod p$

نتيجة: إذا كان p عدداً أولياً وكان a عدداً صحيحاً فإن:

$a^{p} \equiv a \pmod p$

(أ) $p \nmid a$ حسب فيرما يكون:

$a^{p-1} \equiv 1 \pmod p$

نضرب بـ a: $a^{p} \equiv a \pmod p$

(ب) $p \mid a$

$a \equiv 0 \pmod p$

$p \mid a$

$p \mid a^{p} \Rightarrow a^{p} \equiv 0 \pmod p$

وهو المطلوب $a^{p} \equiv a \pmod p$

أي $p \mid a$

$p \mid a(a^{p-1}-1)$

$p \mid (a^p - a) \Rightarrow a^p \equiv a \pmod p$

وهو المطلوب.

ملاحظة: إذا كان $a^n \equiv a \pmod n$ فليس بالضرورة أن يكون n أولياً والعكس صحيح

تمرين للبيت: أثبت أن $5^{38} \equiv 4 \pmod{11}$

أو بيّن أن كان 11 يقسم $11 \mid (5^{38}-4)$ $(5^{10}) \equiv 1 \pmod{11}$

تمرين: إذا كانت p و q عددين أوليين مختلفين وكان

$a^p \equiv a \pmod q$

$a^q \equiv a \pmod p$

وكان $d(a,p)=1$ عندئذ:

$a^{pq} \equiv a \pmod{p.q}$

تمرين (P) حلل العدد 341 بطريقة فيرما.

(C) اثبت أن $2^{340} \equiv 1 \pmod{341}$

$2^{341} \equiv 2 \pmod{341}$

الأعداد التي في هذا الشكل 2^n $n \in \mathbb{Z}$
غير الأولية التي تحقق العلاقة
$2^n \equiv 2 \pmod n$
تدعى أشباه أوليات (أوليات كاذبة)
والعدد (341) هو أول عدد شبه أولي
وبعده (561)

انتهت المحاضرة